National Aeronautics and
Space Administration

NOT MEASUREMENT
SENSITIVE

NASA-STD-2804P
Effective September 4, 2012

MINIMUM INTEROPERABILITY SOFTWARE SUITE

NASA TECHNICAL STANDARD

FOREWORD

This standard is approved for use by NASA Headquarters and all NASA centers and is intended to provide a common framework for consistent practices across NASA programs.

The material covered in this standard is governed and approved by the NASA Information Technology Management Board. Its purpose is to define the baseline software suite necessary to support interoperability both between NASA end user computers and within the NASA operating environment. The standard establishes Client Reference Configurations, Operating System Standards, and Compliance Dates for computers running Microsoft Windows, Apple OS X, and various Linux and UNIX operating systems. Adherence to this standard ensures compliance with Federal requirements for desktop computers, laptops, and other end user devices.

Requests for information, corrections, or additions to this standard should be directed to the John H. Glenn Research Center at Lewis Field (GRC), Emerging Technology and Desktop Standards Group (ETADS), MS 142-4, Cleveland, OH, 44135 or to *desktop-standards@lists.nasa.gov*. This standard may be viewed and downloaded, free of charge, from the NASA Emerging Technology and Desktop Standards web site:

etads.nasa.gov/current/2804.pdf

/signature on file/

Linda Cureton
Chief Information Officer

Table of Contents

1 SCOPE

1.1 Purpose

This standard defines the baseline software suite necessary to support interoperability both between NASA end user computers and within the NASA operating environment. The standard establishes Client Reference Configurations, Operating System Standards, and Compliance Dates for computers running Microsoft Windows, Apple OS X, and various Linux and UNIX operating systems. Adherence to this standard ensures compliance with Federal requirements for desktop computers, laptops, and other end user devices.

1.2 Applicability

Center CIOs will ensure that all NASA employees at their respective centers have access to an interoperable workstation that is equipped with a minimum software suite that meets the standards listed in Section 3 below.

The Client Reference Configuration (CRC) establishes required functionality and required products necessary to meet that functionality. Future procurements intended to address this functionality are restricted to the products defined in the CRC. Existing licenses for other products may not be renewed. Products will be added, replaced, or removed as appropriate to address agency interoperability requirements.

1.3 Waivers

This technical standard is governed by Enterprise Architecture Function as defined in Section 1.2.1.3 of NPR 2800.1B Managing Information Technology. Adherence to this standard ensures compliance with the future state architecture as described in NPR 2830.1 NASA Enterprise Architecture Procedures.

The Emerging Technology and Desktop Standards group, in cooperation with the End User Services Service Executive and the Chief Enterprise Architect, will evaluate and process waivers to this standard as appropriate. Waiver requests will include:

1. the reason the waiver is required,
2. justification for the waiver, and
3. a proposed date by which compliance with the standard will be met.

Waivers will be granted by the NASA CIO or at his/her discretion responsibility will be delegated to the Center or Mission Directorate CIO.

2 ACRONYMS AND DEFINITIONS

2.1 Acronyms

ACES	Agency Consolidated End-User Services
ASCS	Agency Security Configuration Standards
ASUS	Agency Security Update Service CA Certificate Authority
CIO	Chief Information Officer
CIS	Center for Internet Security
CRC	Client Reference Configuration
CSS	Cascading Style Sheets

DAR	Data at Rest (encryption)
ESR	Extended Support Release
ETADS	Emerging Technology and Desktop Standards
FDCC	Federal Desktop Core Configurations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FPKI	Federal Public Key Infrastructure
GnuPG	GNU Privacy Guard
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICA	Independent Computing Architecture
ICAM	Identity Credential Access Management
IDI	ICAM Device Integration
IE	Internet Explorer
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Standards Organization
ITAR	International Traffic in Arms Regulations
IMAP	Internet Message Access Protocol
LTS	Long-term Support
MAPI	Messaging Application Programming Interface
MIME	Multipurpose Internet Mail Extension
NCTR	NASA Client Trust Reference
NEFS	NASA Electronic Forms System
NFCE	NASA Firefox Configuration Extension
NIST	National Institute of Standards and Technology
NOCA	NASA Operational Certificate Authority
NOMAD	NASA Operational Messaging and Directory Service
NSS	Network Security Services
OASIS	Organization for the Advancement of Structured Information Standards
OCIO	Office of the Chief Information Officer
OCS	Microsoft Office Communications Server
PDF	Portable Document Format
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RFC	Request for Comments
RPC	Remote Procedure Call
SBU	Sensitive But Unclassified
SCAP	Security Content Automation Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
USGC	United States Government Configuration Baseline
VPAT	Voluntary Product Accessibility Templates

W3C	World Wide Web Consortium
XHTML	eXtensible HyperText Markup Language
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

2.2 Definitions

2.2.1 Basic Interoperability

Interoperability is the ability to obtain consistent and deterministic results within a specific platform (operating system software, minimum hardware, required and optional software) as well as between platforms (Microsoft, OS X, Linux, Unix) based on the established standards.

2.2.2 Desktop Computer

The term desktop computer is used generically to refer to traditional desktop systems, as well as laptop computers, notebooks, tablets, engineering workstations, and similar platforms that are utilized to provide basic interoperability.

2.2.3 Support for Basic Interoperability

Systems supporting basic interoperability are defined as desktop computers used to exchange information electronically by end users that require any of the functionality listed in Section 3.4, Client Reference Configurations.

3 DETAILED REQUIREMENTS

3.1 Architectural Compliance Requirements

NASA has base-lined and approved the NASA Integrated Information Technology Architecture. The architecture is predicated on:

The selection of standards for a broad and cost-effective infrastructure using commercial off-the-shelf and well-supported open source products to the greatest extent practical − Interoperability both within and external to NASA

Flexibility for future growth − Consistency with generally accepted consensus standards as much as feasible

Security for NASA systems

Among these objectives, ensuring interoperability is one of NASA's most critical issues related to information technology. In many cases, it is in NASA's best interest to specify commercial products as standards for an interoperable implementation of a particular set of related and integrated functions. The products themselves often include additional functionality or proprietary extensions not specified by this standard. While these products can be used to create higher-level interoperability solutions, these solutions may not be recognized within the context of the NASA interoperability environment and may be deprecated without warning by future revisions to this standard. Users of this standard are advised to apply appropriate caution when implementing proprietary or non-standard extensions, features and functions that go beyond the explicitly stated standard functionality.

3.2 Security for NASA systems

The ongoing utility and security of the NASA IT environment is directly dependent on a continuous stream of software (and hardware) updates. All NASA IT service providers must therefore develop processes and solutions which minimize the time required to install updates and new versions of software. This NASA-STD-2804 document will list specific minimum versions of software required for compliance with this standard. Except as specifically indicated, all NASA IT service providers will install minor updates throughout the life-cycle maintenance for the systems, and prepare major new revisions of software (including operating systems and browsers) in the shortest time possible, cognizant with required testing.

It is understood that ingrained legacy processes take some time to change. The above information is provided as a guideline to NASA IT service and application providers that system update cycle times are shortening, and that existing processes are no longer workable.

This version (version P) of NASA-STD-2804 provides notice that the subsequent version of the Standard (version Q), anticipated in the August 2013 time frame, will list the specific Client Reference Configuration software that will be required to participate in the continuous stream of automatic software vendor updates in real time. It is likely that the initial software chosen for this update feature will be individual web browsers, and several of the more security-problematic browser plug-ins and accessory applications. NASA IT service providers should take note of this stated direction and begin the evolution of their system support and application update processes (or alternative environments) during the remainder of 2012 and the first half of 2013, to support an appropriately secure and modernized NASA IT environment.

3.3 Agency Security Configuration Standards

The NASA Office of the Chief Information Officer (OCIO) establishes Agency Federal Information Security Management Act (FISMA) compliance goals and reporting requirements for NASA systems, through the use of NASA System Security Baselines, managed by the Agency Security Configuration Standards (ASCS) Service. OCIO policy requires deployment of the NASA ASCS system configurations to all systems.

The NASA ASCS system security baselines are developed from various sources, including the National Institute of Standards and Technology (NIST) Security Content Automation Program (SCAP) checklists, Center for Internet Security (CIS) Benchmarks, vendor and third-party sources, and are also internally developed by the ASCS staff. These system security baselines, and their associated compliance monitoring measurement content, are managed by ASCS.

NASA Baseline security configurations for each operating system and applicable software listed in this standard can be obtained at

etads.nasa.gov/ascs/

Centers wishing informed local consultation should contact their ASCS Point of Contact, listed here

etads.nasa.gov/ascs/communications

or consult the ASCS web site for additional information.

3.4 Client Reference Configurations

To address application, data, and infrastructure interoperability, and ensure compliance with federally mandated desktop computer configuration settings, the software functionality, applications, interface standards, configuration settings, versions, and deployment settings established by this standard are definitive.

Client Reference Configurations (CRC) are included for each operating system, with the version numbers that were current at the time of this writing, and required configurations listed as appropriate. Current versions of applications shall be used as made available by the application vendor unless specifically stated otherwise. Interface standards are included to guide service providers and system integrators.

The Client Reference Configurations define the operational configuration upon which desktop service providers can define common enterprise images for all interoperable desktops computers. All IT initiatives funded or endorsed by the NASA OCIO presume systems that conform to the Client Reference Configurations. Application service providers and software developers should use the reference configurations to assist with integration and acceptance testing.

The NASA Emerging Technology and Desktop Standards group is working to ensure interoperability at the highest possible revision of products included in the Client Reference Configurations. Applications that meet these interface standards while providing improved end user experience, mitigating security risks, reducing support costs, or offering other tangible improvements may be submitted to standards-comments@lists.nasa.gov for consideration in future revisions to these standards.

3.4.1 Client Reference Configuration for Windows XP

Client Reference Configuration for Windows XP

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Operating System	Windows XP Professional		NASA System Baseline Configuration settings	Service Pack 3 with all security patches	September 30, 2008
Operating System	Windows XP Professional X64 Edition		NASA System Baseline Configuration settings KB968730 Hotfix	Service Pack 2 with all security patches	April 1, 2009
Firewall	Windows Firewall		NASA System Baseline Configuration settings	XP/SP3	September 30, 2008
Smartcard Middleware	ActivIdentity	NIST SP 800-73 Part 3	See section 3.7.1	7.x	September 4, 2012
Data at Rest Full Disk Encryption	Symantec PGP Whole Disk Encryption		Configured to use central policy and key escrow service See section 3.6.5.1		September 4, 2012
Content Encryption	Entrust ESP	S/MIME		9.1.x	September 7, 2010
Secure Email	Entrust ESP	S/MIME		9.1.x	September 7, 2010
Trust Anchor Management	See Section 3.7	FPKI	See Section 3.7	3.5.x	September 4, 2012
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			1.3.x	September 4, 2012
Anti-Virus	Symantec Endpoint Protection		Enterprise update server	12.1.x	September 4, 2012
Anti-Malware	Symantec Endpoint Protection		Enterprise update server	12.1.x	September 4, 2012
Patch Reporting	KBOX	KACE	See section 3.6.4	5.x	September 4, 2012

Client Reference Configuration for Windows XP

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
		Proprietary			
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NFCE v1.3.0 or higher. See section 3.7Recommend automatically install updates	10.x	September 4, 2012
Web Browser	Microsoft Internet Explorer	W3C and industry standards	NASA System Baseline Configuration settings. Also see section 3.7	8.0.x	September 7, 2010
Web Browser	Google Chrome	W3C and industry standards	See section 3.7		September 4, 2012
Office Automation	Microsoft Office (Professional Edition with Outlook)	Office Open XML document format		2010	December 1, 2010
Word Processing	Microsoft Word	Office Open XML document format	Configure to use Office Open XML file format by default	2010	December 1, 2010
Spreadsheet	Microsoft Excel	Office Open XML document format	Configure to use Office Open XML file format by default	2010	December 1, 2010
Presentation	Microsoft PowerPoint	Office Open XML document format	Configure to use Office Open XML file format by default	2010	December 1, 2010
Electronic Mail	Microsoft Outlook	NASA-STD-2815, IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	2010	December 1, 2010
Calendaring	Microsoft Outlook as implemented by NOMAD	iCalendar (RFC 5545)		2010	December 1, 2010

Client Reference Configuration for Windows XP

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Instant Messaging	Office Communicator	SIP	Enterprise OCS Settings as implemented by NOMAD Pidgin-sipe OCS plugin	2007 R2	July 1, 2011
Instant Messaging	Pidgin	XMPP	NASA Jabber Service Pidgin-sipe OCS plugin	2.1.0.x	September 4, 2012
PDF Viewer	Adobe Reader X	PDF		10.1.x	September 4, 2012
Java	Java run-time environment			Java 7	September 4, 2012
Audio/video players	Apple QuickTime Player	Various Multimedia	Default for QuickTime formats	7.7.x	September 4, 2012
Audio/video players	Adobe Flash Player	Flash SWF		11.3.x	September 4, 2012
Audio/video players	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	12.0.x	September 4, 2012
Audio/video players	Silverlight	Various Multimedia		5.0.x	September 4, 2012
Audio/video players	Apple iTunes	Various Multimedia		10.6.x	September 4, 2012
Access to centrally served Windows applications	Citrix Receiver			3.2.x	September 4, 2012
Electronic Forms	FileNet Desktop e-Forms	See Section 3.8	NASA Distribution Center	4.2	June 24, 2008
Video Conferencing	Secure Virtual Team Meeting		nasa.webex.com/		August 2010

3.4.2 Client Reference Configuration for Windows 7

Client Reference Configuration for Windows 7

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Operating System	Windows 7 Enterprise or Ultimate		NASA Baseline Security settings	SP1	August 9, 2011
Operating System	Windows 7 Enterprise or Ultimate X64 Edition		NASA Baseline Security settings	SP1	August 9, 2011
Firewall	Windows Firewall		NASA Baseline Security settings		September 7, 2010
Smartcard Middleware	ActivIdentity ActivClient	NIST SP 800-73 Part 3	See section 3.7.1	7.x	September 4, 2012
Data at Rest Full Disk Encryption	Symantec PGP Whole Disk Encryption		Configured to use central policy and key escrow service See section 3.6.5.1		September 4, 2012
Content Encryption	Entrust	S/MIME		9.1.x	September 7, 2010
Secure Email	Entrust Desktop Solution	S/MIME		9.1.x	September 7, 2010
Trust Anchor Management	See Section 3.7	FPKI	See Section 3.7	3.5.x	September 4, 2012
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			1.3.x	September 4, 2012
Anti-Virus	Symantec Endpoint Protection		Enterprise update server	12.1.x	September 4, 2012
Anti-Malware	Symantec Endpoint Protection		Enterprise update server	12.1.x	September 4, 2012
Patch Reporting	KBOX	KACE Proprietary	See section 3.6.4	5.x	September 4, 2012
Web Browser	Mozilla Firefox	W3C and	NFCE v1.3.0 or higher,	10.x	September 4, 2012

Client Reference Configuration for Windows 7

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
	Extended Support Release	industry standards	see section 3.7Recommend automatically install updates		
Web Browser	Microsoft Internet Explorer	W3C and industry standards	NASA System Baseline Configuration settings. Also see section 3.7	9.0.x	July 1, 2012
Web Browser	Google Chrome	W3C and industry standards	See section 3.7		September 4, 2012
Office Automation	Microsoft Office (Professional Edition with Outlook)	Office Open XML document format		2010	December 1, 2010
Word Processing	Microsoft Word	Office Open XML document format	Configure to use Office Open XML file format by default	2010	December 1, 2010
Spreadsheet	Microsoft Excel	Office Open XML document format	Configure to use Office Open XML file format by default	2010	December 1, 2010
Presentation	Microsoft PowerPoint	Office Open XML document format	Configure to use Office Open XML file format by default	2010	December 1, 2010
Electronic Mail	Microsoft Outlook	NASA-STD-2815, IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	2010	December 1, 2010
Calendaring	Microsoft Outlook as implemented by NOMAD	iCalendar (RFC 5545)		2010	December 1, 2010
Instant Messaging	Communicator	SIP	Enterprise OCS Settings as implemented by NOMAD Pidgin-sipe OCS plugin	2007 R2	August 9, 2011

Client Reference Configuration for Windows 7

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Instant Messaging	Pidgin	XMPP	NASA Jabber Service Pidgin-sipe OCS plugin	2.1.0.x	September 4, 2012
PDF Viewer	Adobe Reader X	PDF		10.1.x	September 4, 2012
Java	Java run-time environment			Java 7	September 4, 2012
Audio/video players	Apple QuickTime Player	Various Multimedia	Default for QuickTime formats	7.7.x	September 4, 2012
Audio/video players	Adobe Flash Player	Flash SWF		11.3.x	September 4, 2012
Audio/video players	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	12.0.x	September 4, 2012
Audio/video players	Silverlight	Various Multimedia		5.0.x	September 4, 2012
Audio/video players	Apple iTunes	Various Multimedia		10.6.x	September 4, 2012
Access to centrally served Windows applications	Citrix Receiver			3.2.x	September 4, 2012
Electronic Forms	FileNet Desktop e-Forms	See Section 3.8	NASA Distribution Center	4.2	June 24, 2008
Video Conferencing	Secure Virtual Team Meeting		nasa.webex.com/		September 7, 2010

3.4.3 Client Reference Configuration for OS X 10.7

Client Reference Configuration for OS X (10.7 Lion)

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Operating System	OS X		CIS Benchmarks with NASA Guidance	10.7.x	April 9, 2012
Firewall	Apple Firewall		Allow essential services Enable firewall loggingEnable Stealth Mode		April 1, 2009
Smartcard Middleware	PIV.tokend		See section 3.7.1 etads.nasa.gov/idi/os-x/		September 4, 2012
PKI	Entrust Secure Desktop for Mac (SDM)	S/MIME	NASA PKI Team specified settings	8.1.x	September 4, 2012
Trust Anchor Management	See Section 3.7	FPKI	See Section 3.7	3.5.x	September 4, 2012
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			1.3.x	September 4, 2012
Anti-Virus	Symantec Endpoint Protection			12.1.x	September 4, 2012
Anti-Malware	Symantec Endpoint Protection			12.1.x	September 4, 2012
Full Disk Encryption	Symantec PGP Whole Disk Encryption		Configured to use central policy and key escrow service See section 3.6.5.1		September 7, 2010
Patch Reporting	KBOX	KACE Proprietary	See section 3.6.4	5.x	September 4, 2012
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	NFCE v1.3.0 or higher, see section 3.7Recommend automatically install updates	10.x	September 4, 2012

Client Reference Configuration for OS X (10.7 Lion)

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Web Browser	Apple Safari	W3C and industry standards	See section 3.7	5.1.x	September 4, 2012
Web Browser	Google Chrome	W3C and industry standards	See section 3.7		September 4, 2012
Office Automation	Microsoft Office 2011 for Mac	Office Open XML document format		2011	April 1, 2011
Word Processing	Microsoft Word 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	14.2.x	December 1, 2010
Spreadsheet	Microsoft Excel 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	14.2.x	December 1, 2010
Presentation	Microsoft PowerPoint 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	14.2.x	December 1, 2010
Electronic Mail	Microsoft Outlook 2011 for Mac	NASA-STD-2815, IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	14.2.x	December 1, 2010
Electronic Mail	Apple Mail	NASA-STD-2815, IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	5.2.x	September 4, 2012
Calendaring	Microsoft Outlook 2011 for Mac as implemented by NOMAD	iCalendar (RFC 5545)		14.2.x	December 1, 2010
Calendaring	Apple iCal	iCalendar (RFC 5545)		5.0.x	September 4, 2012

Client Reference Configuration for OS X (10.7 Lion)

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Instant Messaging	Mac Messenger	SIP	Enterprise OCS Settings as implemented by NOMAD	7.0.x	July 1, 2011
Instant Messaging	Apple iChat	XMPP	NASA Jabber Service	Bundled	June 24, 2008
PDF Viewer	Apple Preview	PDF		5.5.x	September 4, 2012
PDF Viewer	Adobe Reader X	PDF		10.1.x	February 6, 2012
Java	Java run-time environment			Java 7	September 4, 2012
Audio/video players	Apple QuickTime Player	Various Multimedia	Default for QuickTime formats	10.1.x	September 4, 2012
Audio/video players	Adobe Flash Player	Flash SWF		11.3.x	September 4, 2012
Audio/video players	Telestream Flip4Mac WMV	Windows Media	Default for Windows Media	2.4.x	September 4, 2012
Audio/video players	Silverlight	Various Multimedia		5.0.x	September 4, 2012
Audio/video players	Apple iTunes	Various Multimedia	Default for all supported formats	10.6.x	September 4, 2012
Access to centrally served Windows applications	Citrix Receiver			11.5.x	September 4, 2012
Electronic Forms	Adobe Reader X	See Section 3.8		10.1.x	February 6, 2012
Video Conferencing	Secure Virtual Team Meeting		nasa.webex.com/		September 7, 2010

3.4.4 Client Reference Configuration for Linux

Client Reference Configuration for Linux

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise When the operating system vendor provides bundled support for applications included in the CRC, the vendor-provided and supported versions should supersede those of the CRC

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Operating System	Red Hat Enterprise Linux Desktop with Workstation option		CIS Benchmarks with NASA Guidance	5.3 or later	June 24, 2008
Operating System	Ubuntu LTS		CIS Benchmarks with NASA Guidance	12.04.x	September 4, 2012
Firewall	Bundled		Control inbound and outbound connections enabled by default	Bundled	June 24, 2008
Smartcard Middleware	OpenSC		See section 3.7.1See **Error! Hyperlink reference not valid.**		September 4, 2012
Secure Email	Thunderbird	S/MIME	Use exported NOCA certificates	5.0.x	September 4, 2012
Trust Anchor Management	See Section 3.7	FPKI	See Section 3.7	3.5.x	September 4, 2012
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)			1.3.x	September 4, 2012
Anti-Virus	Symantec Antivirus for Linux			1.0.x	September 4, 2012
Data at Rest Encryption	Symantec PGP Whole Disk Encryption		Configured to use central policy and key escrow service		September 4, 2012
Patch Reporting	KBOX	KACE Proprietary	See section 3.6.4	5.x	September 4, 2012
Web Browser	Mozilla Firefox Extended Support Release	W3C and industry standards	See section 3.7Recommend automatically	10.x	September 4, 2012

Client Reference Configuration for Linux

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise When the operating system vendor provides bundled support for applications included in the CRC, the vendor-provided and supported versions should supersede those of the CRC

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
			install updates		
Web Browser	Google Chrome	W3C and industry standards			September 4, 2012
Office Automation	LibreOffice (Ubuntu) OpenOffice (RHEL)	OASIS Open Document Format for Office Applications (Open Document		3.5.x	September 4, 2012
Word Processing	LibreOffice Writer (Ubuntu) OpenOffice (RHEL)	OASIS Open Document Format for Office Applications (Open Document	Configure to use Office Open XML file format by default	3.5.x	September 4, 2012
Spreadsheet	LibreOffice Calc (Ubuntu) OpenOffice (RHEL)	OASIS Open Document Format for Office Applications (Open Document	Configure to use Office Open XML file format by default	3.5.x	September 4, 2012
Presentation	LibreOffice Impress (Ubuntu) OpenOffice (RHEL)	OASIS Open Document Format for Office Applications (Open Document	Configure to use Office Open XML file format by default	3.5.x	September 4, 2012
Electronic Mail	Mozilla Thunderbird(Ubuntu) Evolution (RHEL)	NASA-STD-2815, IMAP4, SMTP, IMAP over SSL/TLS	Configured for access to NOMAD	12.0.x	September 4, 2012
Calendaring	NOMAD Outlook Web Access	iCalendar (RFC 5545)	Web Browser	2.x	June 24, 2008

Client Reference Configuration for Linux

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise When the operating system vendor provides bundled support for applications included in the CRC, the vendor-provided and supported versions should supersede those of the CRC

Functionality	Application	Interface Standard	Required Settings	Version	Effective Date
Instant Messaging	Pidgin	XMPP	NASA Jabber Service	2.9.x	June 24, 2008
PDF Viewer	Adobe Reader			9.4.x	September 4, 2012
Java	Java run-time environment			Java 7	September 4, 2012
Audio/video players	MPlayer	Multimedia	Default for supported formats	1.0.x	June 24, 2008
Audio/video players	Adobe Flash Player	Flash SWF		11.2.x	September 4, 2012
Access to centrally served Windows applications	Citrix Receiver			12.1.x	September 4, 2012
Electronic Forms	FileNet Desktop E-Forms	See Section 3.8		Not supported use Citrix	
Video Conferencing	Secure Virtual Team Meeting		nasa.webex.com/		August 2010

When the operating system vendor provides bundled support for applications included in the CRC, the vendor-provided and supported versions should supersede those of the CRC

3.4.5 Client Reference Configuration for Smartphones and Tablets

Client Reference Configuration for Smartphones and Tablets

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Functionality	Application	Required Settings	Version	Effective Date
Operating System	iOS	CIS Benchmarks with NASA Guidance	5.1 or later	September 4, 2012
Operating System	Android	CIS Benchmarks with NASA Guidance	4.0 or later	September 4, 2012
Operating System	Blackberry	Configured to use Agency Blackberry Enterprise Server	7.1 or later	September 4, 2012

3.4.6 Table of Optional Software for Smartphones and Tablets

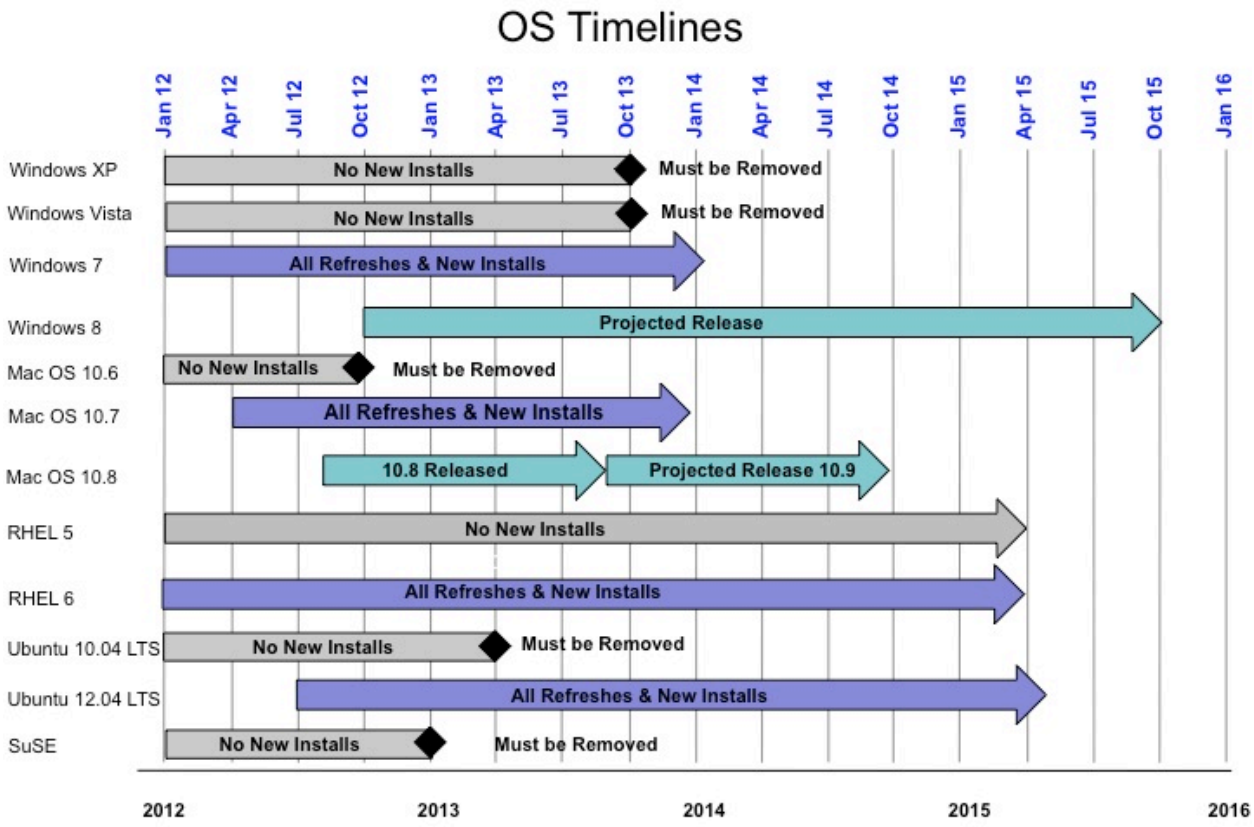
The following table contains optional useful functionality that is not required for interoperability. Where practical, it is recommended that these tools be used rather than similar tools that address the same function. This table often identifies software that may be eventually be included in the Client Reference Configurations. The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Optional Software for Smartphones and Tablets

The versions stated are the versions available at the time of this writing. The current version available from the vendor shall be used unless specifically stated otherwise

Functionality	Application	Version	Effective Date
Access to centrally served Windows applications	Citrix Receiver	5.5.3 or later	September 4, 2012
Video Conferencing	Cisco WebEx	4.0 or later	September 4, 2012
Time & Attendance	WebTADS		

3.5 Operating System Standards, Time Lines, and Compliance Dates



3.5.1 Microsoft Windows

For all versions of the Windows operating system the Windows firewall shall be set to on.

3.5.1.1 Microsoft Windows XP

All Windows XP systems must meet the NASA System Baseline configurations, which ensure compliance with Federal Desktop Core Configuration (FDCC) requirements. Windows XP must be removed from all NASA systems by October 2013.

3.5.1.1.1 Microsoft Windows XP 64-bitWindows XP

Professional x 64 Edition is specified as the standard version of Windows 64 bit for the agency interoperable computing environment and is subject to the Windows XP Client Reference Configuration. Windows XP Professional x 64 Edition must be removed from all NASA systems by October 2013.

3.5.1.2 Microsoft Windows Vista

Microsoft Windows Vista shall not be deployed. Vista must be removed from all NASA systems by October 201

3.5.1.3 Microsoft Windows 7

All Windows 7 systems must meet the NASA Baseline Security Configurations Settings, which ensure compliance with United States Government Configuration Baseline (USGCB) requirements. Microsoft Windows 7 – Enterprise and Ultimate editions only – are approved for deployment. The 64–bit version of Microsoft Windows 7 shall be deployed to all new and refreshed (upgraded) systems. 32–bit versions of Microsoft Windows 7 may be installed if necessary to support non–64 bit capable applications. Existing Windows XP and Vista systems shall be upgraded to either the 64–bit version of Windows 7 or the 32–bit version depending on hardware capability and software dependency. Windows 7 shall be required on all Windows systems by October 2013.

3.5.1.4 Microsoft Windows 8

While no release date has been announced for Windows 8, Microsoft has released a Consumer Preview of Windows 8 that is under evaluation.

3.5.2 OS X

3.5.2.1 OS X 10.7 (Lion)

OS X 10.7 (Lion) is the currently supported operating system on all Intel based interoperable Macintosh systems. At the time of this writing, OS X 10.7.4 is the current maintenance release. OS X 10.7 shall be installed on all Intel based Macs. OS X 10.6 shall be removed immediately. Older versions should be removed from the environment. As always, the operating system must be kept up-to-date with vendor patches.

3.5.2.2 OS X 10.8

OS X 10.8 (Mountain Lion) was released on July 25, 2012. A deployment time line will be established for deployment when interoperability testing is complete.

3.5.3 Linux

Linux systems with no need for interoperability need not comply with the interoperability requirements in this standard. Such systems would include special-purpose computers such as name servers, compute servers, data acquisition systems, special software development workstations, or other components of the overall computing infrastructure. Several product standards are not available for any Linux or UNIX system. In order to comply with this standard, interoperable desktops must have some way to access these products. It is recommended to use the Citrix Receiver client to connect to a Microsoft Windows application server. The Linux distributions that are supported for use on interoperable desktops Red Hat Enterprise Linux Desktop 5 with Workstation option on existing systems. Red Hat Enterprise Linux Desktop 6 with Workstation option on all new and refreshed systems.

www.redhat.com/rhel/desktop

Ubuntu 10.04 LTS (Long-term support) on existing systems. Ubuntu 12.04 LTS (Long-term support) on all new and refreshed systems. Ubuntu 10.04 LTS will be at end of life in April 2013 and must be removed from systems by this date.

www.ubuntu.com/

All new and refreshed Linux systems must run one of the supported Linux distributions. SuSE Linux Enterprise Desktop has been removed from the standard. SuSE Linux users should be migrated to one of the supported Linux distributions.

3.5.4 UNIX

The following UNIX systems are supported in the NASA interoperable computing environment. Generally, both the current version and prior version of the operating system are acceptable. However, the older version of the operating system must continue to be supported by the vendor, and like all systems, must be kept current with security patches.

3.5.4.1 Oracle Solaris/SPARC, x86, and x86-64

Solaris is at version 11. Information about supported Solaris releases may be found at

www.oracle.com/us/products/servers-storage/solaris/index.html - releases

3.5.4.2 3.5.4.2 IBM AIX/POWER

AIX 7.1 is current. AIX versions are described at

www-03.ibm.com/systems/power/software/aix/index.html

3.5.4.3 3.5.4.3 HP HP-UX/PA-RISC

HP-UX 11i v3 is current. The HP-UX 11i web page is at

h71028.www7.hp.com/enterprise/w1/en/os/hpux11i-overview.html

3.6 Additional Client Reference Configuration Guidance

3.6.1 Office Automation Applications

The default document format for Microsoft Office, LibreOffice, and OpenOffice is the ISO Standard Office Open XML format.

As of December 2011, all interoperable Microsoft Windows systems are required to run the 32–bit version of Office 2010 Standard Edition (or better) regardless of processor architecture. The 64–bit version of Office 2010 may be deployed as a point solution, though interoperability problems will likely persist and be uncorrectable.

Microsoft Office 2011 for Mac (Standard Edition) was approved for use December 1, 2010 and is required on all interoperable OS X systems. A Mac version of Outlook replaces Entourage. Note: Office 2011 reinstates support for Visual Basic Applications. LibreOffice is the default Office product for Ubuntu systems.

LibreOffice 3.5 is approved for deployment. OpenOffice is the default Office product for RHEL systems. OpenOffice 3.2 is approved for deployment. Documents created with Microsoft Office do not always render perfectly in LibreOffice or OpenOffice, and vice versa.

3.6.2 Electronic Messaging

NASA has implemented an enterprise-wide electronic messaging service known as NOMAD. This service provides integrated email, calendaring, scheduling, contact management, and instant messaging. All interoperable desktops are required to be configured to access this environment.

Note that while NOMAD is based upon open standards and can support stand-alone email clients that adhere to the defined interface standards of the Client Reference Configurations, utilizing such clients limits end user interoperability, may not be supported by NOMAD, and may result in future inability to participate in the enterprise messaging environment.

Supported Messaging Clients

Windows: Microsoft Outlook

OS X: Microsoft Outlook and Apple Mail

Linux: Mozilla Thunderbird (Ubuntu), Evolution (RHEL)

Apple Mail supports the NOMAD calendar and scheduling environment but does have some integration issues. The choice of client on OS X depends upon the required functionality. In some cases, Microsoft Outlook is more appropriate (for instance, when delegation functionality is required). In other cases Apple Mail and iCal with Address Book are suitable.

Additional clients which conform to the interface standards may be used as point solutions where interoperability might otherwise not be available.

The selection of mail clients will continue to promote secure access to commercial and partner email services in support of extra-Agency (non-NOMAD) collaborative activities.

3.6.3 Web Browsers

Within the last year or so web browser vendors have changed the browser delivery model. The frequency of how often a new version is released has changed from yearly or bi-annually to every 1-2 months. In some cases vendors are managing the release cycle by auto-updating their browser in the background without user intervention or knowledge. Since Mozilla Firefox has moved to a rapid release cycle Mozilla realized that this type of frequent release cycle was not meeting the needs of large organizations. Mozilla offers Firefox Extended Support Release (ESR) to address the needs of large organizations that do not have the agility to remain current with the rapid release cycle.

To avoid inefficiencies and interoperability issues, NASA must adjust to the rapid pace of browser enhancements resulting in new versions from the browser vendors. Web authors, application providers, system integrators, etc., should ensure that their web sites are validated against W3C Markup Validation Service and discontinue the use of checking client browsers for specific versions before granting access.

Due to the rapidly evolving browser environment NASA’s approach to providing interoperable browsers must change. It is understood that legacy processes take some time to change, so to help with the transition to a rapid release, automatic updating browser environment Mozilla Firefox ESR will be replacing the rapid release version of Firefox for applications that require a more stable environment. Mozilla has stated that Firefox ESR will be maintained for a one year period, while providing point releases containing security updates. No new features will be

added to Firefox ESR within this time frame. This should result in a more stable, yet secure browser environment for application vendors.

As always the operating system default browsers such as Internet Explorer for Windows, and Safari for Apple will be supported. If the latest features in a browser are required Google Chrome will be provided to address this market segment. This results in Internet Explorer, Firefox, and Chrome on Windows systems, Safari, Firefox, and Chrome on Macs, and Firefox and Chrome on Linux systems.

For Internet Explorer, and Safari, NASA will maintain support for the most recent production version and the version immediately preceding it. Firefox ESR will be updated with point releases for security updates only. Chrome will automatically update in the background as designed by Google.

Browsers should be configured with the Agency approved list of trust anchors as found in the NASA Client Trust Reference (NCTR). Some browsers will require additional setting, also found at the NCTR site.

etads.nasa.gov/resources/client-trust-reference

Browsers should be configured per ICAM Desktop Integration configuration requirements found at etads.nasa.gov/idi/

For additional information see section 3.7 ICAM Desktop Integration

3.6.3.1 Microsoft Internet Explorer

The NASA System Configuration Baseline must be used for all versions of Microsoft Internet Explorer.

Internet Explorer 7 (IE7) can continue to be used on Windows XP systems until Windows XP is retired in October 2013. The NASA System Configuration Baseline must be used for IE7.

Internet Explorer 8 (IE8) can continue to be used on Windows XP systems until Windows XP is retired in October 2013. The NASA System Configuration Baseline must be used for IE8.

Internet Explorer 9 (IE9) is the standard browser on all interoperable Windows 7 systems. IE9 is not available to systems running Windows XP. IE8 shall be removed from all Vista and Windows 7 systems by July 2012.

3.6.3.2 Mozilla Firefox Extended Support Release (ESR)

Mozilla Firefox (ESR) is offered by Mozilla to address the needs of large organizations that do not have the agility to remain current with the rapid release cycle of modern browsers. The ESR version of Firefox will be maintained by Mozilla for a one year period, while providing point releases containing security updates. No new features will be added to Firefox ESR within this time frame. NASA is supporting Firefox ESR for those applications that require a more stable environment.

3.6.3.3 Apple Safari

Safari 6 is default browser provided by Apple and is standard for all interoperable Macintosh systems. Safari 6.0 or later must be installed. The use of Safari on Windows is not supported.

3.6.3.4 Google Chrome

Google Chrome a popular browser within the industry, and is the browser selected for use when the most recent browser features are needed. The version of Google Chrome shall be maintained by Google's automatic update process.

3.6.4 System Configuration Reporting and Patch Management

The Agency solution for patch management, compliance reporting and system configuration reporting is the Dell Kace product. For current information on the appropriate configuration and patch management client for your system(s), including specific version levels, please refer to the Agency Security Update Service (ASUS) web site at asus.nasa.gov/ Agency policy requires that an reporting client be installed on all systems for which clients are available.

3.6.5 Desktop Encryption

3.6.5.1 Data at Rest (DAR) Encryption

Symantec PGP Desktop is being implemented as the Agency solution for Data at Rest (DAR) encryption. ACES has begun deploying Symantec PGP in order to ensure adherence to NASA and Federal directives. All Agency laptops and desktop computers storing sensitive information will receive DAR. Please contact your local DAR representative for center specific deployment details or visit aces.ndc.nasa.gov/subnav/dar.html for more information.

3.6.5.2 FileVault version 2

With the release of OS X 10.7 FileVault now provides full disk encryption. While recommended for OS X 10.6 systems, the use of FileVault version 2 is required for all NASA OS X 10.7 (and later OS X versions) systems which do not have the Agency Data At Rest (DAR) solution installed. Master keys should be escrowed with Apple when no organizational means is available from the system service provider to organizationally escrow FileVault keys. The marginal risk of data loss for individual self-administered systems is deemed less critical to the Agency than the continued exposure of NASA data on unencrypted end user systems.

3.6.5.3 Content Encryption and Secure Email

NASA maintains a secure desktop solution based on Entrust. The Client Reference Configurations include the appropriate Entrust client for use in encrypting desktop files and folders and Outlook plug-in sending signed, encrypting messages to other NASA employees. Work is constantly underway to extend trust to other Federal Agencies so that secure mail can be exchanged outside of NASA in the future. For situations in which Entrust cannot be used to exchange secure files or messages, the Free Software Foundation's, GNU Privacy Guard (GnuPG) is approved for use and has been added to Table 4.1.1 Table of Optional Software. Note that GnuPG does not meet the rigorous enrollment and certificate management processes inherent with Entrust and cannot provide the authentication assurance levels necessary to meet Federal Government requirements for the exchange of sensitive information. It should therefore only be used as a point solution when Entrust is not an option.

3.7 Desktop ICAM Integration Configuration Requirements

The Identity, Credential and Access Management infrastructure services provide a significant portion of the core NASA operating environment. For proper interoperability with the ICAM services the following additional requirements have been identified.

3.7.1 Authentication Configuration Requirements

The ICAM Desktop Integration team develops software and configuration requirements for authentication with NASA standard operating systems. These configurations support such functions as:

- Smartcard PIV authentication with the NASA badge
- NASA Launchpad Simplified Logon
- Single-Sign-On with Active Directory integrated applications such as SharePoint, Project Server, and Exchange
- Authentication with PIV derived x509 soft-certificate credentials

ICAM Desktop Integration configuration requirements, which includes settings for operating system, browser, and middleware can be found at

etads.nasa.gov/idi/

3.7.2 NASA Client Trust Reference

The NASA Client Trust Reference (NCTR) repository can be found on the ETADS web site at

etads.nasa.gov/resources/client-trust-reference/

Trusted Sites and Certificates are listed in the NCTR when they are approved for deployment on NASA end user systems as required to enable Agency level business functions for groups of personnel appreciably larger than those at any single NASA center.

3.7.2.1 Trusted Sites

The trusted site listing facilitates secure workstation interoperability with applications and services that are both internally and externally provided.

3.7.2.2 Certificates

Operating systems, as well as some third party applications, such as Mozilla Firefox and Mozilla Thunderbird, contain trusted certificate stores. The certificate stores are already preloaded and updated periodically by the product vendors with trusted certificates that are required for standard business functionality. In addition to these vendor-supplied certificates, some of these certificate stores require additional certificates for interoperability with Agency and Agency affiliate services. This collection of additional certificates is managed as part of the NASA Client Trust Reference.

3.7.3 Additional Relying Party Requirements

All client applications that perform PKI operations shall be required to support the SHA-2 family hashing algorithms as of November 2010. Information on SHA-2, RSA, and encryption algorithm lifetimes can be found in NIST special publications SP800-78-2 and SP800-131.

3.8 Electronic Forms

In 2009 the Agency-wide eForms software (FileNet v4.2), used for over 16 years, was decommissioned by the vendor (IBM). The NASA OCIO is taking the necessary steps to replace

the software with a new Agency-wide integrated solution that supports NASA's business practices, embraces technology and innovation, and increases efficiency.

The NASA OCIO purchased an enterprise license for Adobe Reader Extensions (RE) in September 2011, enabling Center form designers to create eligible forms in a PDF format that can be filled and saved, and facilitating the retirement of eligible FileNet versions. Unfortunately, the Adobe RE software alone does not offer the advanced design capability and scripting required to replace all NASA and Center forms currently designed in the FileNet format. Until the Agency procures a new electronic forms solution, the NASA Forms Working Group will continue to develop knowledge articles for the ACES and non-ACES supported machines as a means to provide information on interoperability issues as they are identified and work-arounds as they become available.

In the interim, known FileNet interoperability issues exist for

1. Windows machines using SHA 256 certificates issued after December 2010 to sign FileNet forms, and
2. Mac machines running Lion.

Known Adobe PDF interoperability issues exist for

1. Mac machines using Preview vs. Adobe Reader for PDF forms, and
2. PDF forms completed within a Web browser on Mac and Windows machines.

End users are encouraged to contact their Center Forms Managers to report interoperability issues with both FileNet and Adobe PDF software. Contact information can be found on the NASA Electronic Forms System (NEFS) website

www.nef.nasa.gov

The NEFS web site serves as the central repository of Agency-level forms (created when a form is used by two or more Centers) and Center level forms. The NEFS site is available to NASA Centers and Installations, recognized partners, qualified contractors/service providers, and the general public when doing business with NASA. For the purpose of FileNet form distribution, a distribution center profile has been created to allow access to NASA and Center forms designed using the FileNet software. These profiles are maintained and distributed through the NEFS web site. The design and control of forms (Agency level/NASA forms, Center forms, and organization forms) are addressed in NPD 1420.1A, NASA Forms Management, and available in NODIS.

3.9 Section 508 Compliance Requirements

Software products procured after June 21, 2001 must be in conformance with Section 508 of the Rehabilitation Act. Complete information and guidance on addressing Section 508 requirements is available at www.nasa.gov/accessibility/section508/sec508_overview.html When developing and testing software, users are reminded to use the recommended tools for evaluation.

3.9.1 Section 508 Tools Table

Section 508 Tools			
Function	**Windows**	**OS X**	**Linux**
Screen Reading Software	JAWS 8.x or higher VoiceOverWindow Eyes 6.x or higher Firefox: WebAim's Wave Toolbar Add-on Firefox: WebAim's Wave Toolbar Add-on	VoiceOver	
Desktop Web Browser Tool	Firefox: WebAim's Wave Toolbar Add-onInternet Explorer: Vision Australia's Web Accessibility Toolbar for IE – 2011	Firefox: WebAim's Wave Toolbar Add-onInternet Explorer: Vision Australia's Web Accessibility Toolbar for IE – 2011	Firefox: WebAim's Wave Toolbar Add-onInternet Explorer: Vision Australia's Web Accessibility Toolbar for IE – 2011
PDF Documents	Adobe Acrobat 8.x or higherNetCentric Technologies CommonLook Plug-in for Acrobat	Adobe Acrobat 8.x or higher	

The NASA Emerging Technologies and Desktop Standards team has evaluated vendor-supplied Voluntary Product Accessibility Templates (VPAT) for Windows XP, Windows Vista, Windows 7, OS X Lion, Office 2010, and Firefox and believes that they satisfy the Section 508 requirements to an acceptable degree.

3.10 FIPS 140-2 Compliance Requirements

NASA will adhere to the guidelines and recommendations of the National Institute of Standards and Technology as required by the Federal Information Security Management Act, particularly as they apply to computer security and encryption technology for desktop hardware and software. More specifically, NASA will comply with Federal Information Processing Standards (FIPS) 140-1 and 140-2 as applicable, validated encryption modules become available.

NASA application developers and service providers are reminded that whenever cryptographic-based security systems are used to protect sensitive information in computer systems, the cryptographic modules utilized must be FIPS 140-2 compliant as validated by NIST . A current list of validated products can be found at

csrc.nist.gov/cryptval/

The following products mentioned in NASA-STD-2804 have been validated by a NIST-accredited testing laboratory and may be appropriate to protect sensitive information with cryptography under specific conditions:

FIPS 140-2 Validated Software			
Product	**Validation Module**	**Certification**	**Comments**
Apple FileVault, Safari, Mail	Apple FIPS Cryptographic Module	#1701	Single User Mode, FIPS 140-2
Microsoft	Kernel Mode Cryptographic Module for	#997	Single User Mode, FIPS 140-1

FIPS 140-2 Validated Software			
Product	**Validation Module**	**Certification**	**Comments**
	Windows XP		
Microsoft	Microsoft Windows 7 Cryptographic Primitives Library	#1329	Single User Mode, FIPS 140-2
Microsoft	Windows 7 Enhanced Cryptographic Provider (RSAENH)	#1330	Single User Mode, FIPS 140-2
Microsoft	Windows 7 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)	#1331	Single User Mode, FIPS 140-2
Microsoft Outlook	Outlook Cryptographic Provider	#110	Single User Mode, FIPS 140-1, S/MIME
Entrust PKI Software	Entrust Entelligence Kernel Mode Cryptographic module	#1043	Single User Mode, FIPS 140-2
F-Secure SSH	F-Secure® Cryptographic Library™ for Windows	#437	FIPS 140-2, When operated in FIPS Mode, Single User Mode
F-Secure SSH	F-Secure® Cryptographic Library™ for Linux	#776	FIPS 140-2, When operated in FIPS Mode, Single User Mode
OpenSSL	OpenSSL FIPS Object Module (1.2)	#1111	Single User Mode, FIPS 140-2
Citrix ICA Client for Windows	Kernel Mode Cryptographic Module for Windows XP	Not Validated	Uses MS Windows FIPS Crypto Module
Symantec PGP	PGP Cryptographic Engine	#1684	FIPS 140-2, When operated in FIPS Mode
Mozilla NSS	Network Security Services (NSS)	#1280	FIPS 140-2, When operated in FIPS Mode
Entrust PKI Software	L Version 8.0	#797 #1043	FIPS 140-2, When operated in FIPS Mode

3.11 Wireless Requirements

The current minimum wireless hardware and software configuration that will be used by NASA to support interoperability is defined in NASA-STD-2850.1. For information on the ongoing conditions that wireless infrastructure devices must satisfy to connect to the NASA network see NASA-STD-2850.1 which when posted will be available at standards.nasa.gov/

3.12 Internet Protocol version 6 (IPv6) Requirements

Internet Protocol version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to Internet Protocol version 4 (IPv4). IPv6 is described in Internet standard document RFC 2460 et al.

Most modern day operating systems are IPv6 capable. On Windows systems from Windows Vista onward Microsoft has enabled IPv6 by default. Apple has delivered IPv6 capable systems since OS X 10.2. Both Red Hat Enterprise Linux and Ubuntu Linux are IPv6 capable. Modern cellular LTE networks are natively IPv6.

IPv6 shall be enabled. Detailed information on Federal requirements for IPv6 can be found at the NIST USGv6 Profile and Testing Program.

IPv6 will not replace IPv4 in the near future. Interoperable Agency workstations should continue to provide IPv4 in addition to IPv6 network capability until further notice.

3.13 Energy Management

In order to comply with Executive Order 13423, printers, laptops and desktop systems must be configured to use energy-saving settings.

3.13.1 Computers

Requirements:

- Displays shall be set to sleep after 15 minutes of idle time
- Systems shall go to sleep after 60 minutes of idle time

Wake-on-LAN functionality shall be enabled on all NASA general purpose end user computer systems whose hardware and software support this functionality.

Generally, the level of sleep should be as effective as possible at saving power, given the constraints of the environment. To reduce power consumption to a minimum the S4 power savings mode (hibernate state) shall be used.

Servers and other special-purpose systems are exempted from this requirement.

3.13.2 Printers

All clients shall be configured for duplex printing by default.

3.13.3 Virtualization

Virtualization technology allows multiple operating systems to be run on a single physical computer. If a desktop virtualization product is required for interoperability the recommended solution (VMWare) must be used. See Table of Optional Software. The virus protection software listed in the Client Reference Configuration shall be used with Virtualization products.

3.14 Password Management Tool

As part of the Federal and Agency Identity Credential and Access Management (ICAM) programs, NASA is implementing strong authentication for access to NASA IT systems and applications per the guidance of HSPD-12 and OMB M-11-11 using federally issued PIV smartcards, and eventually PIV-I smartcards provided by authorized issuers. Part of the strategy includes requiring system and application authentication to utilize the central authentication sources, namely the NASA Consolidated Active Directory environment and the NASA Access Launchpad for web application authentication, and to deprecate the use of single factor authentication credentials, namely username and password. While significant progress has been made, smartcard enablement is still being developed in a number of cases. Further, it is

recognized that users require access to a wide array of both Federal and non-Federal IT systems, most outside of NASA's control, which employ password-based authentication mechanisms.

NIST SP 800-63 does not permit local storage of password credentials as such action would reveal the authentication secret to a party (application) other than the claimant (the user) or the verifier operated by the Credential Service Provider (the Federal IT system being accessed). Under no circumstances, shall a smartcard holder's PIV smartcard PIN, or other Federal IT system credentials (including NASA issued RSA token PINs, NCAD account password, and Access Launchpad password), be managed within a consumer retail or other password management tool. For access to non-Federally controlled IT systems, a password management tool is permissible if it has an implementation that is compliant with NPR 2810.1A requirements.

4 ADDITIONAL SOFTWARE TABLES

4.1 Optional Software

The following table contains optional useful functionality that is not required for interoperability. These software applications and utilities can be made available to end users upon request or distributed with standard enterprise images to support interoperability. Where practical, it is recommended that these tools be used rather than similar tools that address the same function. This table often identifies software that may be eventually be included in the Client Reference Configurations.

Table of Optional Software

Function	Windows	OS X	Linux
3279 client	QWS3270	tn3270	tn3270
ssh client	XWin32	bundled	bundled or OpenSSH
sftp client	FileZilla	Cyberduck	bundled or OpenSSH
Advance file archive extractor/creator	WinZip 12	bundled	bundled
Remote access to Windows systems	MS Remote Desktop Connection	MS Remote Desktop Connection	bundled
X window system server	XWin32	Apple X11	bundled
PostScript previewer	Ghostscript	bundled	bundled
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)	NASA Firefox Configuration Extension (NFCE)	NASA Firefox Configuration Extension (NFCE)
PDF creator	Adobe Acrobat, Pro	Adobe Acrobat, Pro	Scribus
PDF writer/converter	PrimoPDF, MS Office 2007 PDF plug-ins	bundled	bundled

Project Management	MS Project 2007	OpenProj	OpenProj
Alternate Cryptographic Software	Gpg4win	GPGTools	GnuPG
Virtualization	VMWare Workstation	VMWare Fusion	VMWare Workstation
Microbloggin/Twitter	TweetDeck	Nambu	Pidgin
Password Management	1Pasword	1Pasword	
Voice-over-Internet Protocol	Skype	Skype	Skype

4.2 Agency Required Software

The following table summarizes software that must be installed on all Agency desktop systems, regardless of their interoperability requirements. This software is included in the Client Reference Configuration.

Agency Required Software				
Function	**Windows**	**OS X**	**Linux**	**Unix**
FISMA compliance	NASA System Configuration Baselines	CIS Benchmarks	CIS Benchmarks	CIS Benchmarks
Patch reporting	KACE KBOX	KACE KBOX	KACE KBOX	KACE KBOX
Anti-Virus	Symantec Endpoint Protection	Symantec Endpoint Protection	Symantec	Symantec
FIPS 201 Authentication	ActivClient	PIV.tokend	OpenSC	OpenS

5 REVIEW AND REPORTING REQUIREMENTS

5.1 Interoperability Maintenance Reporting

Upon request, Center CIOs will provide the NASA CIO with a summary report, outlining the status of minimum interoperability access for each NASA employee.

5.2 Interoperability Reporting

Each Center CIO will utilize the Agency selected processes and tools, both manual and automated, to report on an annual basis to the NASA CIO the hardware and software configuration of all workstations at their respective Centers. The report will contain sufficient information to ascertain if each workstation supports NASA employees or is Government-furnished equipment to a contractor, whether the equipment is required to be interoperable, and a description of the hardware architecture/environment. The report will specify the number of NASA employees that do not have access to interoperable workstations.

5.3 Basic Interoperability Standards Maintenance

This standard, and its companion, NASA-STD-2805 Minimum Hardware Configurations, are maintained on behalf of the NASA CIO by the Emerging Technology and Desktop Standards group. Together, these standards define the software, hardware, and configurations necessary to ensure basic interoperability within the NASA information technology computing infrastructure. This standard will be reviewed and updated on an as-required basis, not to exceed 12-month intervals. Participation in the revision process is open to all NASA employees. Details on how to be alerted of changes to the standards and/or comment on proposed updates can be found at etads.nasa.gov/ This site also maintains interim guidance, position papers, software and hardware reviews, recommendations and other documentation intended to promote standardized basic interoperability.

6 DURATION

6.1 Duration

This standard will remain in effect until canceled or modified by the NASA CIO.

7 SUPPORTING DOCUMENTS

7.1 Supporting Documents

Supporting documents and additional information related to this standard may be found at etads.nasa.gov/dcs